

1 Chief Judge Ricardo S. Martinez  
2  
3  
4  
5  
6  
7  
8  
9

10  
11 UNITED STATES DISTRICT COURT FOR THE  
12 WESTERN DISTRICT OF WASHINGTON  
13 AT SEATTLE  
14

15 UNITED STATES OF AMERICA,  
16 Plaintiff,  
17  
18 v.  
19  
20 DENYS IARMAK,  
21 Defendant.  
22

23 NO. CR19-257RSM  
24  
25 **PLEA AGREEMENT**

26  
27  
28 The United States of America, by and through undersigned counsel, and  
Defendant DENYS IARMAK, and his attorney, Charles Kaser, enter into the following  
Agreement, pursuant to Federal Rule of Criminal Procedure 11(c)(1)(A) and (B):

1. **Charges.** Defendant, having been advised of the right to have this matter  
tried before a jury, agrees to waive that right and enters a plea of guilty to the following  
charges contained in the Indictment:

a. Conspiracy to Commit Wire Fraud, as charged in Count 1, in  
violation of Title 18, United States Code, Section 1349.

b. Conspiracy to Commit Computer Hacking, as charged in Count 16,  
in violation of Title 18, United States Code, Section 371.

1 By entering these pleas of guilty, Defendant hereby waives all objections to the  
 2 form of the charging document. Defendant further understands that before entering his  
 3 guilty pleas, he will be placed under oath. Any statement given by Defendant under oath  
 4 may be used by the United States in a prosecution for perjury or false statement.

5 The United States agrees to seek dismissal of Counts 2 to 15, and 17 to 26 at the  
 6 time of sentencing.

7 **2. Elements of Offenses.** The elements of the offenses to which Defendant is  
 8 pleading guilty are as follows:

9 a. The elements of Conspiracy to Commit Wire Fraud, as charged in  
 10 Count 1, in violation of Title 18, United States Code, Section 1349, are as follows:

11 First, two or more persons, in some way or manner, agreed to try to  
 12 accomplish a common and unlawful plan to commit a fraud crime listed in Title 18  
 13 Chapter 63, as charged in the indictment, namely, Wire Fraud, in violation of Title 18,  
 14 United States Code, Section 1343; and

15 Second, the defendant knew the unlawful purpose of the plan and willfully  
 16 joined in it.

17 The elements of Wire Fraud, are as follows:

18 First, the defendant knowingly participated in a scheme or plan to defraud,  
 19 or a scheme or plan for obtaining money or property by means of false or fraudulent  
 20 pretenses, representations, or promises, or omitted facts;

21 Second, the statements made or facts omitted as part of the scheme were  
 22 material; that is, they had a natural tendency to influence, or were capable of influencing,  
 23 a person to part with money or property;

24 Third, the defendant acted with the intent to defraud, that is, the intent to  
 25 deceive and cheat; and

26 Fourth, the defendant used, or caused to be used, an interstate or foreign  
 27 wire communication to carry out or attempt to carry out an essential part of the scheme.

b. The elements of Conspiracy to Commit Computer Hacking, as charged in Count 16, in violation of Title 18, United States Code, Section 371, are as follows:

First, there was an agreement between two or more persons to commit at least one crime as charged in the indictment, namely, Accessing a Protected Computer in Furtherance of Fraud, in violation of Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A); and, Intentional Damage To a Protected Computer, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and 1030(c)(4)(B)(i);

Second, the defendant became a member of the conspiracy knowing of at least one of its objects and intending to help accomplish it; and

Third, one of the members of the conspiracy performed at least one overt act for the purpose of carrying out the conspiracy.

The elements of Accessing a Protected Computer in Furtherance of Fraud, are as follows:

First, the defendant knowingly accessed without authorization, or exceeded authorized access to, a computer used in or affecting interstate or foreign commerce or communication, or located outside the United States but using it in a manner that affected interstate or foreign commerce or communication of the United States;

Second, the defendant did so with the intent to defraud;

Third, by accessing the computer without authorization, or exceeding authorized access to the computer, the defendant furthered the intended fraud; and,

Fourth, the defendant by accessing the computer without authorization, or exceeding authorized access to the computer, obtained anything of value.

The elements of Intentional Damage to a Protected Computer, are as follows:

First, the defendant knowingly caused the transmission of a program, a code, a command, or information to a computer;

1                   Second, as a result of the transmission, the defendant intentionally impaired  
 2 without authorization the integrity or availability of data, a program, a system, or  
 3 information;

4                   Third, the computer was used in or affected interstate or foreign commerce  
 5 or communication, or located outside the United States but was used in a manner that  
 6 affects interstate or foreign commerce or communication of the United States; and,

7                   Fourth, the offense caused (i) loss to one or more persons during a 1-year  
 8 period aggregating at least \$5,000.00 in value, or (ii) damage affecting 10 or more  
 9 protected computers during a 1-year period.

10                 3. **The Penalties.** Defendant understands that the statutory penalties  
 11 applicable to the Offenses to which he is pleading guilty are as follows:

12                 a.         For the offense of Conspiracy to Commit Wire Fraud, as charged in  
 13 Count 1: A maximum term of imprisonment of up to twenty (20) years, a fine of up to  
 14 \$250,000.00, a period of supervision following release from prison of up to three (3)  
 15 years, and a mandatory special assessment of one hundred dollars (\$100).

16                 b.         For the offense of Conspiracy to Commit Computer Hacking, as  
 17 charged in Count 16: A maximum term of imprisonment of up to five (5) years, a fine of  
 18 up to \$250,000.00, a period of supervision following release from prison of up to three  
 19 (3) years, and a mandatory special assessment of one hundred dollars (\$100).

20                 If a probationary sentence is imposed, the probation period can be for up to five  
 21 (5) years. Defendant agrees that the special assessment shall be paid at or before the time  
 22 of sentencing.

23                 Defendant understands that supervised release is a period following imprisonment  
 24 during which he will be subject to certain restrictive conditions and requirements.  
 25 Defendant further understands that if supervised release is imposed and he violates one or  
 26 more of the conditions or requirements, Defendant could be returned to prison for all or  
 27 part of the term of supervised release that was originally imposed. This could result in  
 28

1 Defendant's serving a total term of imprisonment greater than the statutory maximum  
 2 stated above.

3 Defendant understands that as a part of any sentence, in addition to any term of  
 4 imprisonment and/or fine that is imposed, the Court may order Defendant to pay  
 5 restitution to any victim of the offense, as required by law.

6 Defendant further understands that a consequence of pleading guilty may include  
 7 the forfeiture of certain property either as a part of the sentence imposed by the Court, or  
 8 as a result of civil judicial or administrative process.

9 Defendant agrees that any monetary penalty the Court imposes, including the  
 10 special assessment, fine, costs, or restitution, is due and payable immediately and further  
 11 agrees to submit a completed Financial Statement of Debtor form as requested by the  
 12 United States Attorney's Office.

13 **4. Immigration Consequences.** Defendant recognizes that pleading guilty  
 14 may have consequences with respect to Defendant's immigration status if Defendant is  
 15 not a citizen of the United States. Under federal law, a broad range of crimes are grounds  
 16 for removal, and some offenses make removal from the United States presumptively  
 17 mandatory. Removal and other immigration consequences are the subject of a separate  
 18 proceeding, and Defendant understands that no one, including Defendant's attorney and  
 19 the Court, can predict with certainty the effect of a guilty plea on immigration status.  
 20 Defendant nevertheless affirms that Defendant wants to plead guilty regardless of any  
 21 immigration consequences that Defendant's guilty pleas may entail, even if the  
 22 consequence is Defendant's mandatory removal from the United States.

23 **5. Rights Waived by Pleading Guilty.** Defendant understands that by  
 24 pleading guilty, he knowingly and voluntarily waives the following rights:

- 25       a. The right to plead not guilty and to persist in a plea of not guilty;
- 26       b. The right to a speedy and public trial before a jury of his peers;
- 27       c. The right to the effective assistance of counsel at trial, including, if  
 28 Defendant could not afford an attorney, the right to have the Court appoint one for him;

1                   d.     The right to be presumed innocent until guilt has been established  
2 beyond a reasonable doubt at trial;  
3                   e.     The right to confront and cross-examine witnesses against Defendant  
4 at trial;  
5                   f.     The right to compel or subpoena witnesses to appear on his behalf at  
6 trial;  
7                   g.     The right to testify or to remain silent at trial, at which trial such  
8 silence could not be used against Defendant; and  
9                   h.     The right to appeal a finding of guilt or any pretrial rulings.

10                6.     **United States Sentencing Guidelines.** Defendant understands and  
11 acknowledges that the Court must consider the sentencing range calculated under the  
12 United States Sentencing Guidelines and possible departures under the Sentencing  
13 Guidelines together with the other factors set forth in Title 18, United States Code,  
14 Section 3553(a), including: (1) the nature and circumstances of the offenses; (2) the  
15 history and characteristics of Defendant; (3) the need for the sentence to reflect the  
16 seriousness of the offenses, to promote respect for the law, and to provide just  
17 punishment for the offenses; (4) the need for the sentence to afford adequate deterrence to  
18 criminal conduct; (5) the need for the sentence to protect the public from further crimes  
19 of Defendant; (6) the need to provide Defendant with educational and vocational training,  
20 medical care, or other correctional treatment in the most effective manner; (7) the kinds  
21 of sentences available; (8) the need to provide restitution to victims; and (9) the need to  
22 avoid unwarranted sentence disparity among defendants involved in similar conduct who  
23 have similar records. Accordingly, Defendant understands and acknowledges that:

24                a.     The Court will determine Defendant's Sentencing Guidelines range  
25 at the time of sentencing;  
26                b.     After consideration of the Sentencing Guidelines and the factors in  
27 18 U.S.C. § 3553(a), the Court may impose any sentence authorized by law, up to the  
28 maximum term authorized by law;

1                   c.     The Court is not bound by any recommendation regarding the  
 2 sentence to be imposed, or by any calculation or estimation of the Sentencing Guidelines  
 3 range offered by the parties or the United States Probation Department, or by any  
 4 stipulations or agreements between the parties in this Plea Agreement; and

5                   d.     Defendant may not withdraw a guilty plea solely because of the  
 6 sentence imposed by the Court.

7                   7.     **Ultimate Sentence.** Defendant acknowledges that no one has promised or  
 8 guaranteed what sentence the Court will impose.

9                   8.     **Restitution.** The parties agree that they will recommend that the Court  
 10 apportion liability for restitution owed to all victims of the criminal conduct committed  
 11 by the criminal organization charged in the conspiracies described herein, including the  
 12 fraud loss on card issuers, financial institutions, breached victim companies, insurance  
 13 companies, cardholders, and vendor businesses. Defendant agrees to pay restitution in  
 14 the apportioned amount of \$2,000,000.00 (which shall not be joint and several with any  
 15 other FIN7 defendant). Said amount shall be due and payable immediately and shall be  
 16 paid in accordance with a schedule of payments as proposed by the United States  
 17 Probation Office and ordered by the Court.

18                   9.     **Forfeiture of Assets.** Defendant agrees, pursuant to Title 18, United States  
 19 Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), to forfeit  
 20 to the United States, immediately, all of his right, title, and interest in any and all  
 21 property, real or personal, which constitutes or is derived from proceeds traceable to the  
 22 offense set forth in Count 1 of the Indictment, and includes, but is not limited to, a sum of  
 23 money in the amount of \$100,000, representing proceeds Defendant personally obtained,  
 24 directly or indirectly, as a result of Defendant's commission of the offense charged in  
 25 Count 1 of the Indictment

26                   Defendant understands and acknowledges that the sum of money the United States  
 27 seeks to forfeit is separate and distinct from the restitution that is ordered in this case.

1       Defendant further agrees, pursuant to Title 18, United States Code, Sections  
 2 982(a)(2)(B) and 1030(i), to forfeit to the United States, immediately, all of his right,  
 3 title, and interest in any and all property constituting, or derived from, proceeds  
 4 Defendant obtained, directly or indirectly, as the result of the offense set forth in Count  
 5 16 of the Indictment, and further to forfeit Defendant's interest in any personal property  
 6 that was used, or intended to be used, to commit, or to facilitate the commission of, that  
 7 offense, including but not limited to the following:

- 8       a.       One (1) laptop identified as FBI evidence item 1B222.
- 9       b.       One (1) silver Dell XPS laptop, bearing no. 2RR74H2, with charger,  
 10 identified as FBI evidence item 1B208.
- 11       c.       One (1) black Xiaomi A1 cell phone, with a note labeled "password:  
 12 19871988", identified as FBI evidence item 1B207.
- 13       d.       Two (2) Sandisk Micro Chip 16 GIGABYTE Motorola MicroSD  
 14 cards, identified as FBI evidence item 1B206.
- 15       e.       One (1) Sandisk 32 GIGABYTE thumbdrive, identified as FBI  
 16 evidence item 1B205.
- 17       f.       One (1) black Xiaomi A2 cell phone, with a note labeled "password:  
 18 007700", identified as FBI evidence item 1B204.
- 19       g.       One (1) Sandisk Cruzer Blade 64 GIGABYTE thumbdrive,  
 20 identified as FBI evidence item 1B203.
- 21       h.       One (1) phone/laptop charging cord, identified as FBI evidence item  
 22 1B202.

23       Defendant agrees to fully assist the United States in the forfeiture of the above-  
 24 described property and to take whatever steps are necessary to pass clear title to the  
 25 United States, including but not limited to: surrendering title and executing any  
 26 documents necessary to effectuate such forfeiture; assisting in bringing any assets located  
 27 outside the United States within the jurisdiction of the United States; and taking whatever  
 28 steps are necessary to ensure that assets subject to forfeiture are not sold, disbursed,

1 wasted, hidden, or otherwise made unavailable for forfeiture. Defendant agrees not to  
 2 file a claim to any of the above-described property in any federal forfeiture proceeding,  
 3 administrative or judicial, which may be or has been initiated.

4 The United States reserves its right to proceed against any remaining property not  
 5 identified in this Plea Agreement, including any property in or over which Defendant has  
 6 any interest or control, if that property is subject to forfeiture under any federal statute.

7 **10. Abandonment of Contraband/Property.** Defendant agrees that if any  
 8 federal law enforcement agency seized any firearms, ammunition, firearm accessories, or  
 9 contraband that were in Defendant's direct or indirect control, Defendant abandons any  
 10 and all interest in those assets and consents to their federal administrative disposal,  
 11 official use, and/or destruction by the federal law enforcement agency that seized them.  
 12 Defendant further agrees to abandon his interest in, and consents to the destruction of, the  
 13 electronic devices, and any data contained within, identified in this agreement, including  
 14 paragraph 9, above.

15 **11. Statement of Facts.** The parties agree on the following facts. Defendant  
 16 admits he is guilty of the charged offense or offenses:

17 a. Defendant Denys Iarmak is a Ukrainian national and has used various  
 18 aliases and nicknames, including, but not limited to "Denys Yarmak," "Denys Jarmak,"  
 19 as well as "GakTus" and "gt." As discussed below, Defendant Iarmak, while residing in  
 20 Ukraine, was a member of a sophisticated foreign-based hacking operation that targeted  
 21 victims in the United States and elsewhere.

22 b. From approximately November 2016 through November 2018, Defendant  
 23 Iarmak was a member of a financially motivated hacking group commonly referred to as  
 24 "FIN7." Since at least August 2015, and continuing through Defendant's arrest, FIN7  
 25 launched attacks against hundreds of U.S. companies in an effort to breach the network  
 26 security of those victims and to steal financial information and non-public information.  
 27 FIN7 consists of dozens of experienced computer specialists located in multiple  
 28 countries. As discussed below, Defendant knowingly and intentionally entered into an

1 agreement with other members of FIN7 to gain unauthorized access to protected  
 2 computers and servers of hundreds of protected computer networks located in the  
 3 Western District of Washington, and elsewhere in the United States, with the goal of  
 4 stealing financial information that could then be sold for financial gain.

5       c.     One of FIN7's primary objectives was to steal payment card information  
 6 from victim companies. FIN7 stole information for tens of millions of payment cards  
 7 from U.S. companies, and then offered that stolen information for sale, including for sale  
 8 on underground forums such as Joker Stash. That payment card information typically  
 9 included the payment card number, the name of the payment cardholder, and the zip code  
 10 in which the card was used, among other data. FIN7 members understood that the stolen  
 11 payment card data would be used to conduct fraudulent transactions across the United  
 12 States and in foreign countries.

13       d.    FIN7 used a front company called Combi Security to recruit hackers and to  
 14 provide a veil of legitimacy to the illegal enterprise. Combi Security portrayed itself as a  
 15 legitimate computer security company that provided penetration-testing services to a  
 16 variety of companies around the world. On its public website, Combi Security presented  
 17 itself as "one of the leading international companies in the field of information security."  
 18 In truth and fact, Combi Security carried out no legitimate work, and was not hired by  
 19 any company to provide security-related services.

20       e.    FIN7 carried out its attacks primarily through the use of phishing emails  
 21 and the use of social engineering techniques to encourage the recipients of the phishing  
 22 emails to inadvertently activate malware contained in or attached to the emails. Once  
 23 activated, the malware would connect a compromised victim computer to a network of  
 24 command and control servers located around the world. Through its command and  
 25 control infrastructure, FIN7 would upload additional malware onto victim computers,  
 26 conduct surveillance, and otherwise maintain remote control of victim computers. After  
 27 breaching a particular victim's computer, FIN7 would use that computer to establish a  
 28 foothold in the victim's network, and then move laterally through the network to locate

1 sensitive financial information, such as payment card information, that could be stolen  
 2 and monetized.

3 f. Among other targets, FIN7 sought to locate point-of-sale (“POS”) systems  
 4 through which it could remotely upload malware onto POS terminals that were used to  
 5 process payment card transactions at thousands of retail and commercial locations across  
 6 the United States. FIN7 then used the malware to scrape and exfiltrate the payment card  
 7 information. In doing so, FIN7 caused to be transmitted in interstate and foreign  
 8 commerce, numerous wire communications and electronic commands, including  
 9 communications and commands to POS terminals located in the Western District of  
 10 Washington.

11 g. Defendant Iarmak served as a high-level hacker, whom the group referred  
 12 to as a “pentester,” and was directly involved in breaching the networks of numerous  
 13 prominent U.S. businesses. He was involved in various aspects of the scheme, including,  
 14 but not limited to, the design and creation of phishing emails, with the embedded  
 15 malware payloads, as well as the intrusion of victim company networks and the  
 16 exfiltration of stolen data, including payment card information.

17 h. One means of private communication used by FIN7 members is Jabber.  
 18 Jabber is an instant messaging service that allows members to communicate through a  
 19 privately hosted server. Defendant Iarmak and his various co-conspirators used Jabber to  
 20 coordinate hacking efforts. For instance, among the numerous Jabber communications  
 21 made in furtherance of the conspiracy:

22 i. On or about December 26, 2016, Defendant Iarmak provided  
 23 another member of the cybercriminal group with his bank information in order to receive  
 24 payments.

25 ii. On or about April 28, 2017, Defendant Iarmak described the  
 26 creation and use of phishing emails to and another member of the cybercriminal group,  
 27 specifically, how to create and test the malware payload for a phishing email.

iii. On or about July 24, 2017, Defendant Iarmak discussed and exchanged stolen victim information with another member of the cybercriminal group.

iv. On or about October 20, 2017, Defendant Iarmak shared the stolen user credentials for an employee of a victim company.

i. FIN7 conspirators, including Defendant Iarmak, also frequently used project management software such as JIRA, hosted on private virtual servers in various countries, to coordinate their malicious activity and to manage the assorted network intrusions. JIRA is a project management and issue-tracking program used by software development teams. JIRA allows team members to create “projects” containing posted “issues” under which other team members can make comments and share data. Under each issue, FIN7 members would track their progress breaching the victim’s security, upload data stolen from the victim, and provide guidance to each other. As but one example, Defendant Iarmak created a JIRA issue, to which he and other members of the cybergroup had access, for a specific victim company, and, on or about March 3, 2017, Defendant Iarmak updated that JIRA and uploaded data he had stolen from that company.

j. FIN7 members, including Defendant Iarmak, were aware of reported arrests of other FIN7 members, but nevertheless continued to attack U.S. businesses. Moreover, while Defendant Iarmak was working for FIN7, a number of companies publicly reported that they had suffered data breaches involving the theft of payment card information that were later attributed to FIN7. For example, Chipotle (Victim-3) publicly disclosed a data breach that impacted approximately 3.9 million payment cards, and Jason's Deli (Victim-6) publicly disclosed a data breach that impacted approximately 2 million payment cards.

k. During the course of the scheme, Defendant received compensation for his participation in FIN7, which far exceeds comparable legitimate employment in Ukraine. For the purposes of this Plea Agreement, the parties agree that – during Defendant’s participation in the malware scheme – FIN7 illegal activity resulted in over \$100 million in losses to financial institutions, merchant processors, insurance companies, retail companies, and individual cardholders. These losses included, *inter alia*, costs associated

1 with fraudulent purchases made with the stolen payment card information, replacing  
 2 compromised payment cards, removing FIN7's malware from compromised systems, and  
 3 responding to law enforcement requests for information in connection with this  
 4 prosecution. In addition, FIN7 caused loss to 10 or more victim companies by breaching  
 5 the victim companies' network security that far exceed \$5,000 in each year from 2016 to  
 6 2019.

7       1. On about November 29, 2019, Defendant Iarmak was arrested by Thai  
 8 police in Bangkok, Thailand. At the time, he was in possession of electronic devices,  
 9 including a silver Dell XPS laptop computer (with hard drives), electronic storage  
 10 devices, and mobile phones, described in paragraph 9, above, which contained evidence  
 11 relevant to the scheme. For instance, those and other devices included data and other  
 12 information linking Defendant Iarmak to known FIN7 nicknames and other  
 13 communications about his employment at FIN7 and references to avoiding law  
 14 enforcement.

15       The parties further agree that the Court may consider additional facts contained in  
 16 the Presentence Report (subject to standard objections by the parties) and/or that may be  
 17 presented by the United States or Defendant at the time of sentencing, and that the factual  
 18 statement contained herein is not intended to limit the facts that the parties may present to  
 19 the Court at the time of sentencing.

20       12. **Sentencing Factors.** The parties agree that the following United States  
 21 Sentencing Guidelines ("USSG") provisions apply to this case:

22           a.      A base offense level of 7, pursuant to USSG § 2B1.1(a)(1).  
 23           b.      An offense level enhancement of 30 levels (+30), based on a loss  
 24 amount of more than \$550,000,000, pursuant to USSG § 2B1.1(b)(1)(P). For the  
 25 purposes of this Plea Agreement, the parties agree to limit the number of stolen payment  
 26 cards to 20 million, which represents the approximate number of unique card numbers  
 27 recovered to date. Pursuant to Application Note 3(F)(i), a \$500 loss amount is imputed to  
 28

1   || each payment card, resulting in a total loss amount, for Guidelines purposes, of \$10  
2   || billion.

12 f. An offense level enhancement of 2 levels (+2), because the offense  
13 involved the trafficking in unauthorized access devices and counterfeit access devices  
14 and because the offense involved the possession of more than 5 means of identification  
15 that were unlawfully obtained, pursuant to USSG § 2B1.1(b)(11).

16 g. An offense level reduction for acceptance of responsibility, as set  
17 forth in paragraph 12, below, conditioned upon Defendant's fulfillment of the  
18 requirements stated at USSG § 3E1.1.

19 h. Defendant's Guidelines range is 25 years, because the statutory  
20 authorized sentence is less than the minimum of the applicable Guidelines range,  
21 pursuant to USSG § 5G1.1.

22 The parties agree they are free to present arguments regarding the applicability of  
23 all other provisions of the United States Sentencing Guidelines. Defendant understands,  
24 however, that at the time of sentencing, the Court is free to reject these stipulated  
25 adjustments, and is further free to apply additional downward or upward adjustments in  
26 determining Defendant's Sentencing Guidelines range.

27       13. **Acceptance of Responsibility.** At sentencing, *if* the district court  
28 concludes Defendant qualifies for a downward adjustment for acceptance of

1 responsibility pursuant to USSG § 3E1.1(a) and the defendant's offense level is 16 or  
 2 greater, the United States will make the motion necessary to permit the district court to  
 3 decrease the total offense level by three (3) levels pursuant to USSG §§ 3E1.1(a) and (b),  
 4 because Defendant has assisted the United States by timely notifying the United States of  
 5 his intention to plead guilty, thereby permitting the United States to avoid preparing for  
 6 trial and permitting the Court to allocate its resources efficiently.

7 **14. Non-Prosecution of Additional Offenses.** As part of this Plea Agreement,  
 8 the United States Attorney's Office for the Western District of Washington and the  
 9 Computer Crime and Intellectual Property Section of the United States Department of  
 10 Justice agree to dismiss other pending counts at the time of sentencing and agree not to  
 11 prosecute Defendant for any additional offenses known to it as of the time of this  
 12 Agreement that are based upon evidence in its possession at this time, and that arise out  
 13 of the conduct giving rise to this investigation. In this regard, Defendant recognizes the  
 14 United States has agreed not to prosecute all of the criminal charges the evidence  
 15 establishes were committed by Defendant solely because of the promises made by  
 16 Defendant in this Agreement. Defendant agrees, however, that for purposes of preparing  
 17 the Presentence Report, the United States Attorney's Office will provide the United  
 18 States Probation Office with evidence of all conduct committed by Defendant.

19 Defendant agrees that any charges to be dismissed before or at the time of  
 20 sentencing were substantially justified in light of the evidence available to the United  
 21 States, were not vexatious, frivolous or taken in bad faith, and do not provide Defendant  
 22 with a basis for any future claims under the "Hyde Amendment," Pub. L. No. 105-119  
 23 (1997).

24 **15. Breach, Waiver, and Post-Plea Conduct.** Defendant agrees that, if  
 25 Defendant breaches this Plea Agreement, the United States may withdraw from this Plea  
 26 Agreement and Defendant may be prosecuted for all offenses for which the United States  
 27 has evidence. Defendant agrees not to oppose any steps taken by the United States to  
 28 nullify this Plea Agreement, including the filing of a motion to withdraw from the Plea

1 Agreement. Defendant also agrees that, if Defendant is in breach of this Plea Agreement,  
 2 Defendant has waived any objection to the re-institution of any charges that previously  
 3 were dismissed or any additional charges that had not been prosecuted.

4 Defendant further understands that if, after the date of this Agreement, Defendant  
 5 should engage in illegal conduct, or conduct that violates any conditions of release or the  
 6 conditions of confinement (examples of which include, but are not limited to, obstruction  
 7 of justice, failure to appear for a court proceeding, criminal conduct while pending  
 8 sentencing, and false statements to law enforcement agents, the Pretrial Services Officer,  
 9 Probation Officer, or Court), the United States is free under this Plea Agreement to file  
 10 additional charges against Defendant or to seek a sentence that takes such conduct into  
 11 consideration by requesting the Court to apply additional adjustments or enhancements in  
 12 its Sentencing Guidelines calculations in order to increase the applicable advisory  
 13 Guidelines range, and/or by seeking an upward departure or variance from the calculated  
 14 advisory Guidelines range. Under these circumstances, the United States is free to seek  
 15 such adjustments, enhancements, departures, and/or variances even if otherwise  
 16 precluded by the terms of the Plea Agreement.

17 **16. Waiver of Appellate Rights and Rights to Collateral Attacks.**

18 Defendant acknowledges that, by entering the guilty pleas required by this plea  
 19 agreement, Defendant waives all rights to appeal from Defendant's conviction and any  
 20 pretrial rulings of the Court. Defendant further agrees that, provided the Court imposes a  
 21 custodial sentence that is within or below the Sentencing Guidelines range (or the  
 22 statutory mandatory minimum, if greater than the Guidelines range) as determined by the  
 23 Court at the time of sentencing, Defendant waives to the full extent of the law:

24 a. Any right conferred by Title 18, United States Code, Section 3742,  
 25 to challenge, on direct appeal, the sentence imposed by the Court, including any fine,  
 26 restitution order, probation or supervised release conditions, or forfeiture order (if  
 27 applicable); and

b. Any right to bring a collateral attack against the conviction and sentence, including any restitution order imposed, except as it may relate to the effectiveness of legal representation.

This waiver does not preclude Defendant from bringing an appropriate motion pursuant to 28 U.S.C. § 2241, to address the conditions of Defendant's confinement or the decisions of the Bureau of Prisons regarding the execution of Defendant's sentence.

If Defendant breaches this Plea Agreement at any time by appealing or collaterally attacking (except as to effectiveness of legal representation) the conviction or sentence in any way, the United States may prosecute Defendant for any counts, including those with mandatory minimum sentences, that were dismissed or not charged pursuant to this Plea Agreement.

17. **Voluntariness of Plea.** Defendant agrees that Defendant has entered into this Plea Agreement freely and voluntarily, and that no threats or promises were made to induce Defendant to enter a plea of guilty other than the promises contained in this Plea Agreement or set forth on the record at the change of plea hearing in this matter.

18. **Statute of Limitations.** In the event this Plea Agreement is not accepted by the Court for any reason, or Defendant breaches any of the terms of this Plea Agreement, the statute of limitations shall be deemed to have been tolled from the date of the Plea Agreement to: (1) thirty (30) days following the date of non-acceptance of the Plea Agreement by the Court; or (2) thirty (30) days following the date on which a breach of the Plea Agreement by Defendant is discovered by the United States Attorney's Office.

11

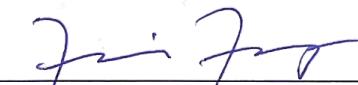
11

1       19. **Completeness of Agreement.** The United States and Defendant  
2 acknowledge that these terms constitute the entire Plea Agreement between the parties,  
3 except as may be set forth on the record at the change of plea hearing in this matter. This  
4 Agreement binds only the United States Attorney's Office for the Western District of  
5 Washington and the Computer Crime and Intellectual Property Section of the United  
6 States Department of Justice. It does not bind any other United States Attorney's Office  
7 or any other office or agency of the United States, or any state or local prosecutor.

8  
9       Dated this 19 day of November, 2021.

10  
11       /s/ Denys Iarmak  
12       DENYS IARMAK  
13       Defendant

14       /s/ Charles Kaser  
15       CHARLES KASER  
16       Attorney for Defendant

17         
18       FRANCIS FRANZE-NAKAMURA  
19       STEVEN MASADA  
20       Assistant United States Attorneys

21         
22       ANTHONY TEELUCKSINGH  
23       Trial Attorney, Computer Crime and Intellectual  
24       Property Section, Department of Justice